State of Arizona

Department of Economic Security Information Technology Standards	Title: 1-38-0045 Computer and Application Systems Authentication Policy	
***Subject*:** This policy defines authentication methods that must be used when accessing DES systems.	***Effective Date:*** 04/03/03	***Revision:*** 1.2

1. Summary of Policy Changes

1.1. **10/29/04** - Addition by the DTS Information Security Administration of 6.5, about employees' authentication from a remote site, and that vendors must also enforce strong two-factor authentication when hosting DES data.

1.2. **05/01/06 –** Section 6 rewritten with changes to reflect updates in policy and technology.

2. Purpose

This policy defines authentication methods that must be used by DES employees and all others with access to DES IT computer or application systems.

3. Scope

This policy applies to all DES administrative entities, councils, divisions, administrations, and programs.

4. Responsibilities

4.1. The DES Director, Deputy Directors, Associate Director, and Assistant Directors are responsible for implementing and enforcing this policy.

4.2. The DES CIO and the DES Division of Technology Services are responsible for implementing this policy.

4.3. All DES Managers and Supervisors are responsible for monitoring compliance to this policy.

4.4 ISA shall initially approve any exceptions to this policy. Final approval shall be done by the appropriate DES Assistant Director and the DES CIO before it may be implemented.

4.5 Other uses of PKI may be implemented with the prior approval of the appropriate DES Assistant Director and the DES CIO.

5. Definitions and Abbreviations

5.1. Definitions

5.1.1. **PKI – P**ublic **K**ey **I**nfrastructure enables users of a non-secure public network, such as the Internet, to securely exchange data through the use of a public and a private cryptographic key pair that is obtained and shared through a trusted authority. PKI provides for a digital certificate that can identify an individual or an organization and directory services that can store and, when necessary, revoke the certificates.

5.1.2. **VPN –** A **V**irtual **P**rivate **N**etwork is a way to use a public telecommunication infrastructure, such as the Internet, to provide remote offices or individual users with secure access to their organization's network.

5.1.3. **SecurID Fob –** SecurID is a proprietary authentication technology that uses a small electronic device called a "fob". The fob displays a password that changes periodically, and is synchronized with a password generator in the network at the authentication point.

5.2. Abbreviations

5.2.1. **ADOA– A**rizona **D**epartment **o**f **A**dministration

5.2.1. **CIO – C**hief **I**nformation **O**fficer

5.2.2. **DTS – D**ivision of **T**echnology **S**ervices

5.2.3. **DES – D**epartment of **E**conomic **S**ecurity

5.2.4. **GITA – G**overnment **I**nformation **T**echnology **A**gency

5.2.5 **ISA – I**nformation **S**ecurity **A**dministration

5.2.6. **PC – P**ersonal **C**omputer

5.2.7 **CISO – C**hief **I**nformation **S**ecurity **O**fficer

6. Policy

6.1 A password is required for authentication on all DES computer and applications systems on the intranet. In some cases, secondary authentication is required (see section 7.0).

6.2 Password requirements

6.2.1 It is forbidden for a user to reveal a password to anyone else. Procedures for user support shall be designed such that it is never necessary for anyone to know someone else's password after initial assignment.

6.2.2 Users must not be able to re-use a password for a history of six passwords. Administrators must not be able to re-use a password for a history of six passwords.

6.2.3 All passwords must contain at least two alphabetic (at least one must be upper and one must be lowercase) and one non-alphabetic (numeric) character. Non-alphabetic characters include only numbers (0-9). The use of control characters and other non-printing characters is prohibited because they may inadvertently cause network transmission problems or unintentionally invoke certain system utilities.

6.2.4 All users must be automatically forced to change their passwords at least once every thirty (30) days. All administrator passwords must be changed every thirty (30) days.

6.2.5 To protect against password guessing attacks, the number of consecutive attempts to enter an incorrect password must be strictly limited. After three unsuccessful attempts to enter a password, the involved user-ID must be either: (a) suspended for thirty minutes, or (b) if dial-up or other external network connections are involved, disconnected.

6.3 A common directory service (DS) shall be used as the user authentication database for access to all DES systems where access control is required.

6.4 Application systems (built internally or purchased) must examine technical feasibility of using the common DS method. Incompatible systems may be approved as an exception. Refer to DES 1-38-0002.

6.5 **Secondary authentication -** All remote access to DES systems, with the exception of the Public accessing DES websites, requires a second level of authentication.

6.5.1 All external users must authenticate via one central directory service.

6.5.2 Use of a second level of authentication to authenticate clients entering applications through the Internet shall be approved by the CISO only on an exception basis.

6.5.3 Application Service Provider's are required to use primary and secondary authentication when DES data is accessed by users.

6.5.4 Public Key Infrastructure (PKI) is the approved mechanism for identification and authentication.

6.6 Costs for secondary authentication devices, such as PKI certificates and SecurID“fobs ” must be controlled by DES. DES will control the security devices used by other agencies, stakeholders, and the Public, but may charge those users for the service.

7. Implications

Costs for secondary authentication.

8. Implementation Strategy

All DES business entities should immediately begin to comply with this policy.

9. References

9.1 1-38-0088	Computer and Application Systems Delegation of Trust Policy
9.2 1-38-0086	Computer and Application Systems Identification Policy
9.3 1-38-0087	Computer and Application Systems Authorization Policy
9.4 1-38-0005	Remote Access Authentication Standard
9.5 1-38-0002	DES Information Technology (IT) Standards Compliance Procedure

10. Attachments

None

11. Associated GITA IT Standards or Policies

None

12. **Review Date**

This document will be reviewed twelve (12) months from the original adoption date and every twelve months thereafter.